

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 25 nov. 2010

"L'entreprise dans les nuages ... et face aux subversions"



CAMILLE
H A A S
ET FILS



Le "cloud computing" ou informatique en nuages est un état de l'art qui oblige à rester les pieds sur terre!

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 25 nov. 2010

"L'entreprise dans les nuages ... et face aux subversions"

Le cyberspace

***un enjeu stratégique
pour la gendarmerie nationale***

***par le Général d'armée
Marc WATIN-AUGOUARD***

Inspecteur général des armées - gendarmerie



Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 25 nov. 2010

"L'entreprise dans les nuages et face aux subversions"



CAMILLE
H. A. A. S
ET FILS



... Il se couchait sur le dos et regardait courir les nuages... il s'intéressait au petit nuage que le gros venait de dévorer... (R. Rolland, Jean-Christophe, L'aube, p. 21)

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 25 nov. 2010

"L'entreprise dans les nuages ... et face aux subversions"

L'informatique en nuages ou "cloud computing"

***un enjeu pour l'entreprise et
un défi majeur pour la sécurité***

Email : guinier@acm.org

par Daniel GUINIER

Dr ès Sciences, Certifications CISSP, ISSMP, ISSAP, MBCI

Expert judiciaire honoraire près la Cour d'Appel de Colmar

Expert devant la Cour Pénale Internationale de La Haye

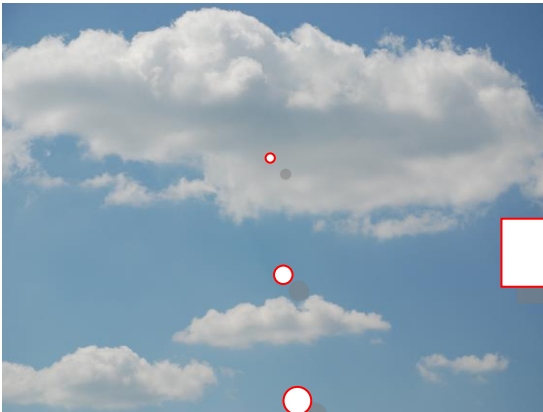
Lieutenant-colonel (RC) de la gendarmerie nationale



Les nuages... et le "cloud computing"

□ ...métaphore météorologique de l'informatique ?

Cumulus



Cumulonimbus



Orage



Cloud computing ?

L'entreprise doit disposer d'une compréhension d'ensemble avant de s'engager dans "les nuages" à long terme dans les meilleures conditions, en connaissance des avantages et des risques.

Les fondements du "cloud computing"

**Guinier D. (2010) : L'informatique dématérialisée en nuages - *Ontologie et sécurité du "cloud computing"*.
Revue "Expertises", octobre , n° 351, pp. 335-344.**

Vocabulaire français ayant cours

□ Evolution du vocabulaire officiel

- "Cloud computing" est traduit par "**Information en nuage**"
(Publication au J.O. n° 0096 du 24 avril 2010)
- "Cloud computing" est traduit par "**Informatique en nuage**"
(Publication au J.O. n° 0129 du 6 juin 2010)

□ Définition officielle du "cloud computing"

Mode de **traitement des données** d'un client, dont l'exploitation s'effectue **par l'Internet**, sous la forme de **services fournis** par un prestataire

"L'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients".

L'informatique "en nuages"

□ **Définition** du "*cloud computing*" ou *informatique "en nuages"*

Modèle d'**informatique dématérialisée** permettant l'accès via un réseau et **sur demande** à un **ensemble partagé de ressources** configurables : réseaux, serveurs, stockage, applications, etc., réparties "*en nuages*" à **divers endroits**

□ **Propriétés**

- virtualisation et distribution des technologies
- flexibilité, minimum d'interaction et d'effort de gestion
- rapidité de fourniture des mises à jour

L'informatique "en nuages" relève de caractéristiques essentielles et comporte plusieurs types de services et modes de déploiement.

Caractéristiques principales

□ Accès

- en libre service à la demande
- à coût plus ou moins réduit
- à grande échelle via les grands réseaux, *tel l'Internet*

□ Ressources

- partagées par une mise en commun
- indépendantes et géographiquement distribuées
- virtuelles pour assurer la compartimentation

□ Services

- souples
- homogènes
- quantifiables

Pour être considérés "en nuages" les services doivent être déployés en respectant les caractéristiques principales. La migration impose alors une préparation minutieuse et une évolution progressive.

Services de base et quelques offres

❑ SaaS : Software as a Service

- les applications sont délivrées via un navigateur

❑ PaaS : Platform as a Service

- les applications sont déployées via une interface

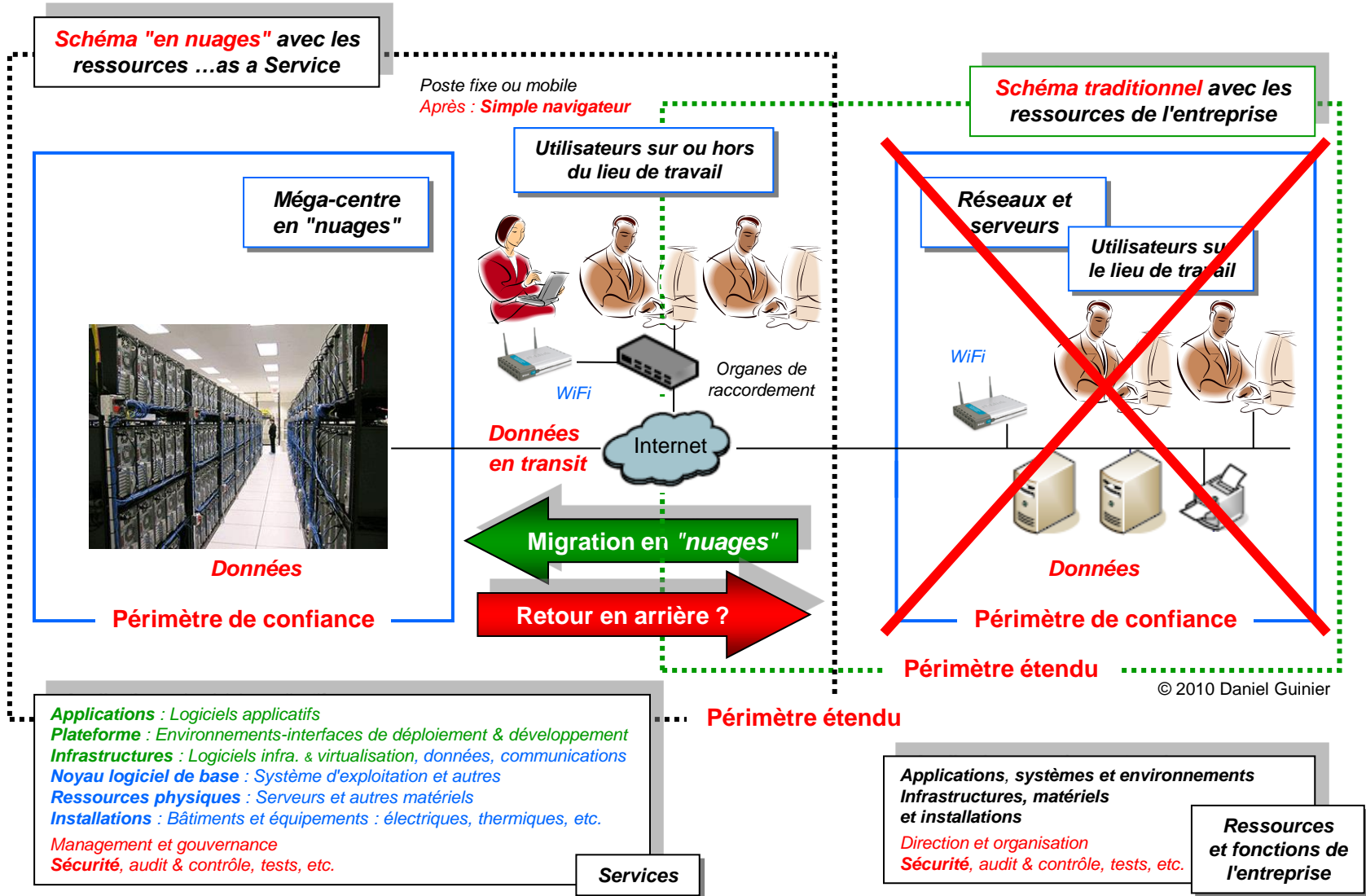
❑ IaaS : Infrastructure as a Service

- les ressources fondamentales sont louées

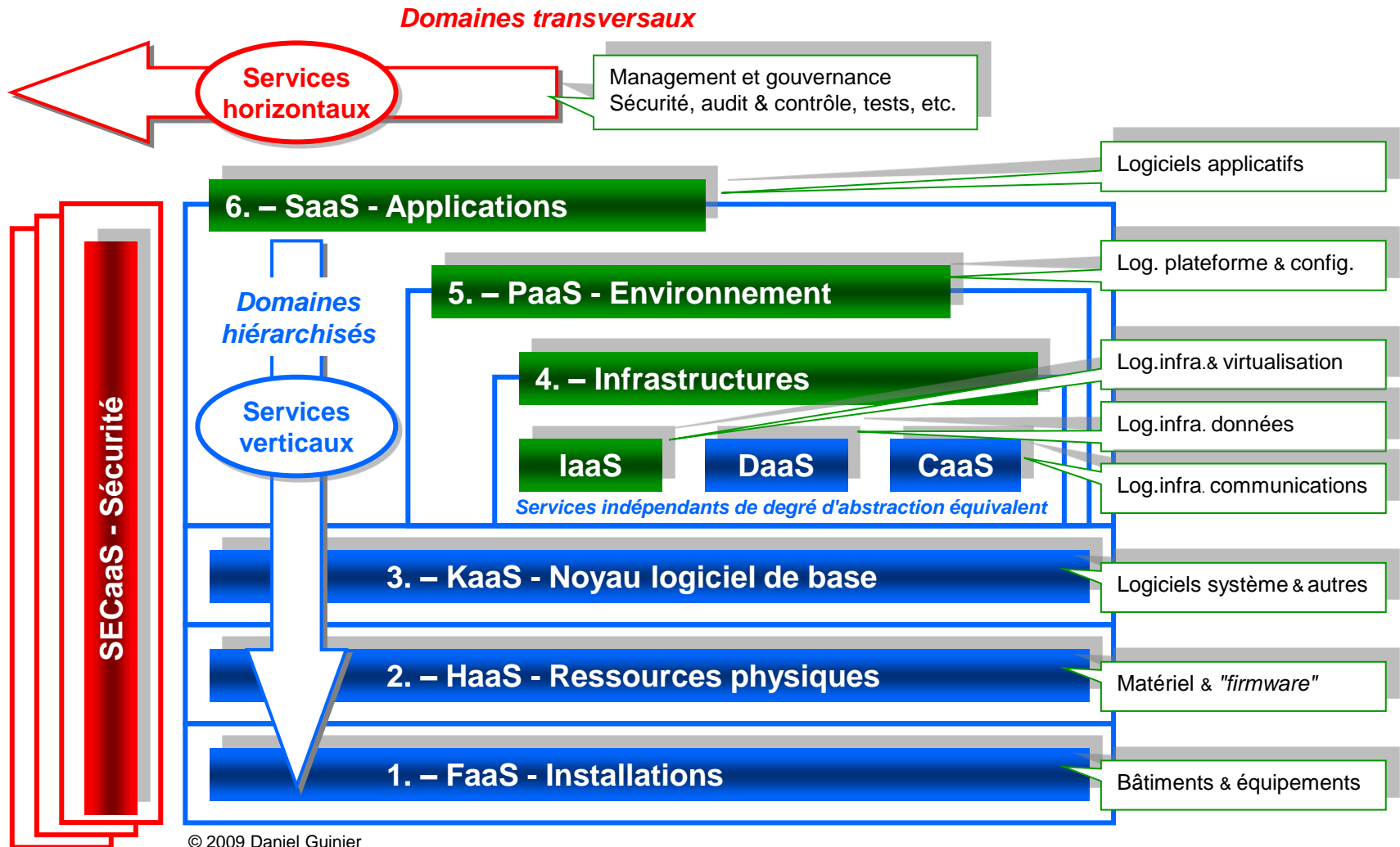
"SPI"	SaaS	PaaS	IaaS
en tant que service	Application logicielle fournie en tant que service et délivrée en configuration fixe	Plateforme de déploiement fournie en tant que service pour déploiement "en nuages"	Infrastructure fournie louée en tant que service : serveur, stockage, réseau, etc.
Quelques offres	<i>Google Apps (Wave, Docs), IBM (Lotus Live), ClusterSeven, Salesforce, Success Metrics, Net Suite, etc.</i>	<i>Google (AppEngine, BigTable), Amazon SQS, Microsoft (Biz Talk, Azure), IBM (Tivoli CMC, Blue Cloud), Citrix (Xen Cloud Platform), etc.</i>	<i>Amazon (S3, EBS, EC2), Nirvanix, Open Nebula, Mosso Cloud, AppNexus, Eucalyptus, Elestra, etc.</i>

Le partage des ressources, la virtualité et la territorialité imposent des garanties à contractualiser, notamment en matière de standards, de migration et de sécurité.

Schémas traditionnel et "en nuages"



Modèle général des services étendus



© 2009 Daniel Guinier

Domaines transversaux et couches complémentaires au modèle SPI.

Modes de déploiement

☐ Privé

- Infrastructure de l'entreprise *ou*
- Infrastructure louée mais sans partage

☐ Souverain

- Infrastructure exclusivement déployée de façon contrôlée sur le territoire national

☐ Communautaire

- Infrastructure partagée par un groupement spécifique

☐ Public

- Infrastructure à grande échelle accessible au public

☐ Hybride

- Infrastructure composée d'au moins deux de ces modes

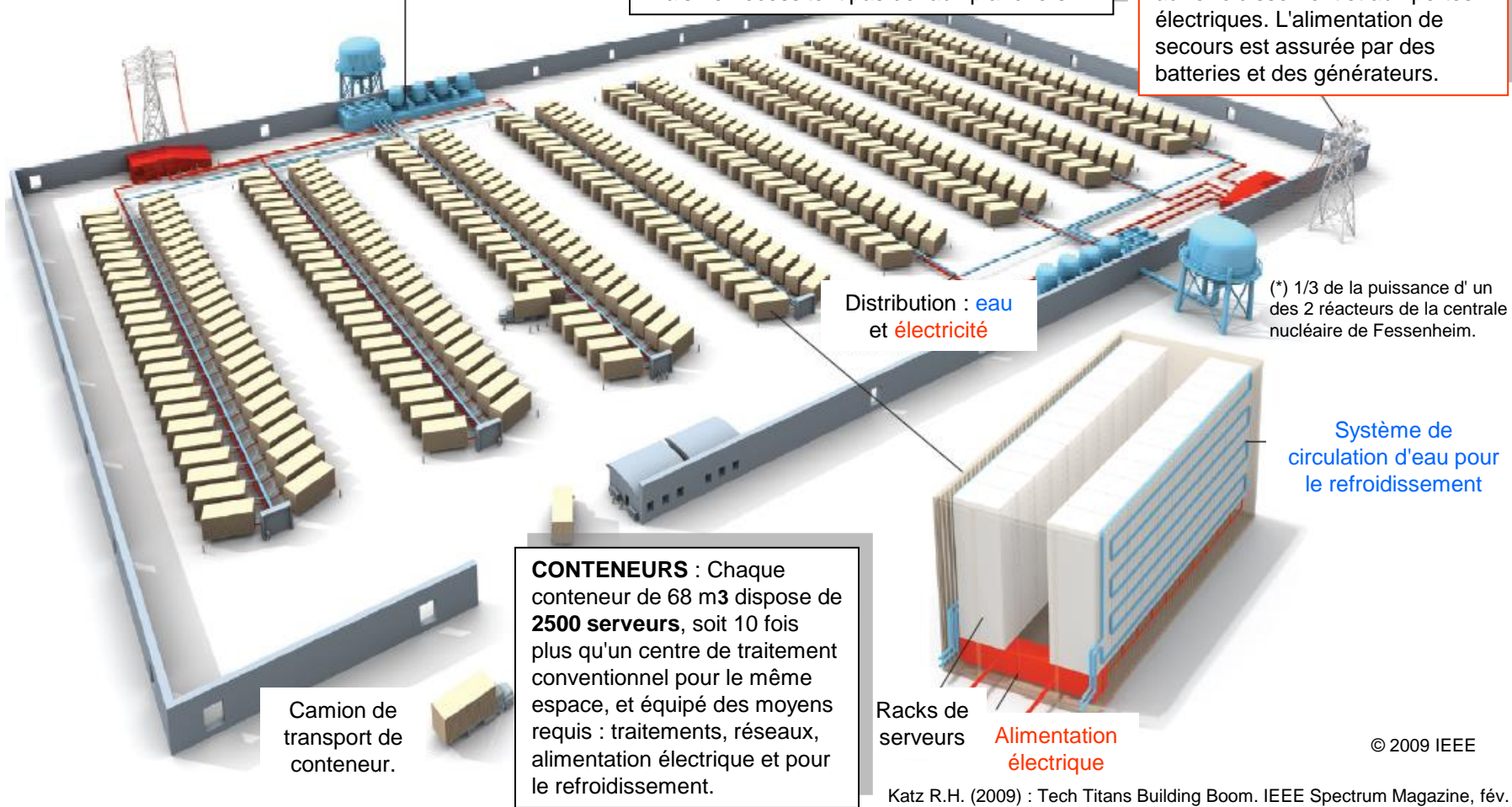
La migration est attendue par étapes pour l'adoption des services et du mode de déploiement : virtualisation, expérimentation, architecture évolutive, sélection d'un environnement, validation de l'ensemble.

Méga-ferme d'un million de serveurs !

REFROIDISSEMENT : Système à haute efficacité à circulation d'eau au travers des conteneurs ; moins consommateur d'énergie que les réfrigérateurs et ne nécessitant pas de salles climatisées.

STRUCTURE : Installations réparties sur **2,4 ha pour 400 conteneurs** livrés par camions. Ils disposent de la connectivité réseau, de l'alimentation électrique, et de la circulation d'eau pour le refroidissement, mais ne nécessitent pas de faux planchers.

ALIMENTATION ELECTRIQUE : Deux sous-stations fourniront **une puissance de 300 MW (*)** au centre de traitement : 200 MW destinés aux serveurs et 100 MW au refroidissement et aux pertes électriques. L'alimentation de secours est assurée par des batteries et des générateurs.



Distribution : eau et électricité

(*) 1/3 de la puissance d'un des 2 réacteurs de la centrale nucléaire de Fessenheim.

Système de circulation d'eau pour le refroidissement

Camion de transport de conteneur.

CONTENEURS : Chaque conteneur de 68 m³ dispose de **2500 serveurs**, soit 10 fois plus qu'un centre de traitement conventionnel pour le même espace, et équipé des moyens requis : traitements, réseaux, alimentation électrique et pour le refroidissement.

Racks de serveurs
Alimentation électrique

© 2009 IEEE

Katz R.H. (2009) : Tech Titans Building Boom. IEEE Spectrum Magazine, fév.

Deux exemples concrets actuels

□ Google

Un des centres de Google près de The Dalles (OR) depuis 2006, apparaît selon un modèle voisin, avec **2 bâtiments sur le même site**, au bord de la rivière Columbia pour disposer d'**eau de refroidissement**.



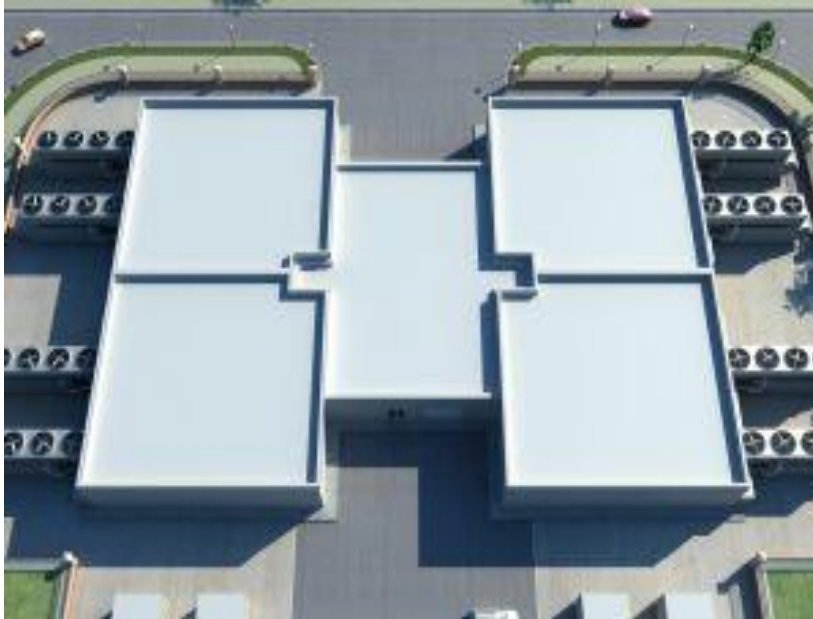
La stratégie de Google se fonde ici sur l'efficacité énergétique et la redondance, avec des grappes de machines à moins de mille dollars

□ Microsoft

Un des centres de Microsoft à Quincy (WA), s'étend sur plus de **4,4 ha**, il dispose d'une puissance de **48 MW**, soit l'équivalent à délivrer pour 40 000 foyers américains, avec **965 km** de fils électriques et 4,8 km de tuyauterie pour le **refroidissement à eau**.

Des constructions en "Legos"...

- Concept de "Flexible Data Center" de type "Lego"



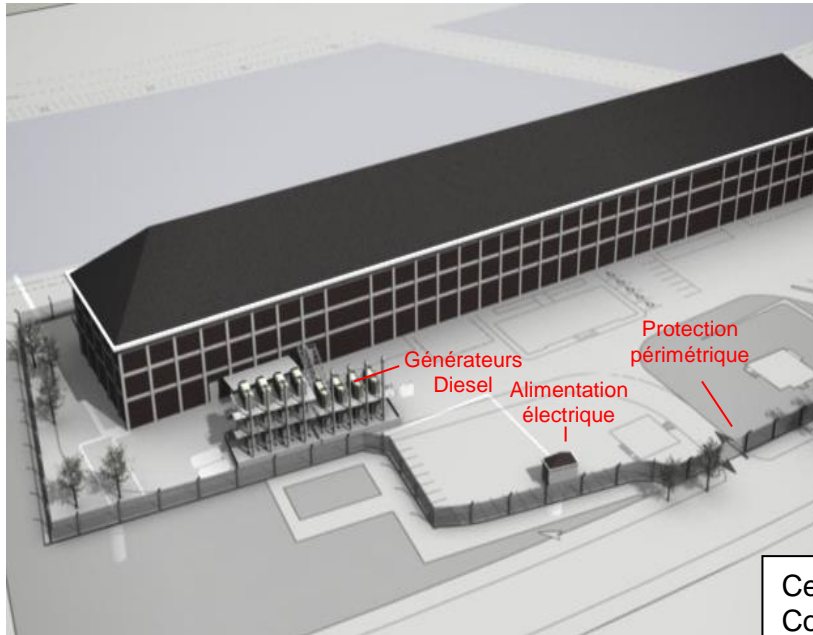
Le concept de "*Flexible Data Center*" de HP relève de la construction rapide et économique de centres de stockage de données

Réf. : <http://www.lemondeinformatique.fr/actualites/lire-des-datacenters-metalliques-de-type-lego-chez-hp-31279.html>

Les éléments préfabriqués standards sont assemblés sur site à la manière de pièces de "Lego", pour répondre au mieux aux besoins de l'entreprise dans une perspective de flexibilité et d'évolution.

Des constructions existantes ...

□ Concept de "Data Center Vert"



Réf. : <http://www.datadock.eu/fr/tour.php>

Le concept de "*Data Center Vert*" relève de la **valorisation** de 2007 à 2010 d'un ancien entrepôt portuaire et du refroidissement à l'eau tirée de puits réduisant la **consommation** d'énergie.

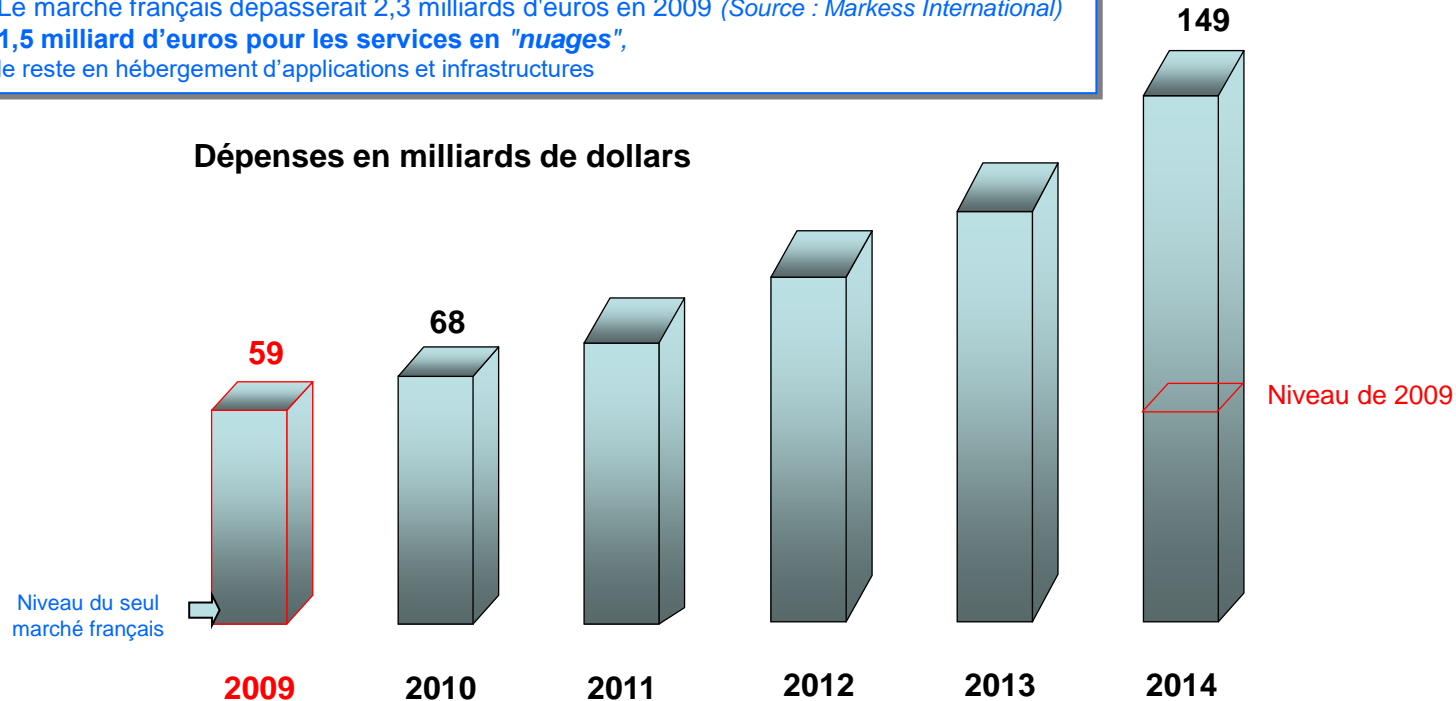
Ce premier aboutissement relève d'actions menées par Alsace Connexia, SFR Collectivités, Alsace International et l'ADIRA, l'agence de développement économique du Bas-Rhin.

Un bâtiment de 22 000 m² a été retenu à Strasbourg par l'hébergeur allemand PlusServer AG qui a déjà investi 17 millions d'euros pour aménager son "Datadock" de 4 200 m², en envisageant 10 000 m².

Dynamisme du marché des services

□ Dépenses mondiales de services "en nuages" prévues

Le marché français dépasserait 2,3 milliards d'euros en 2009 (Source : Markess International)
1,5 milliard d'euros pour les services en "nuages",
le reste en hébergement d'applications et infrastructures



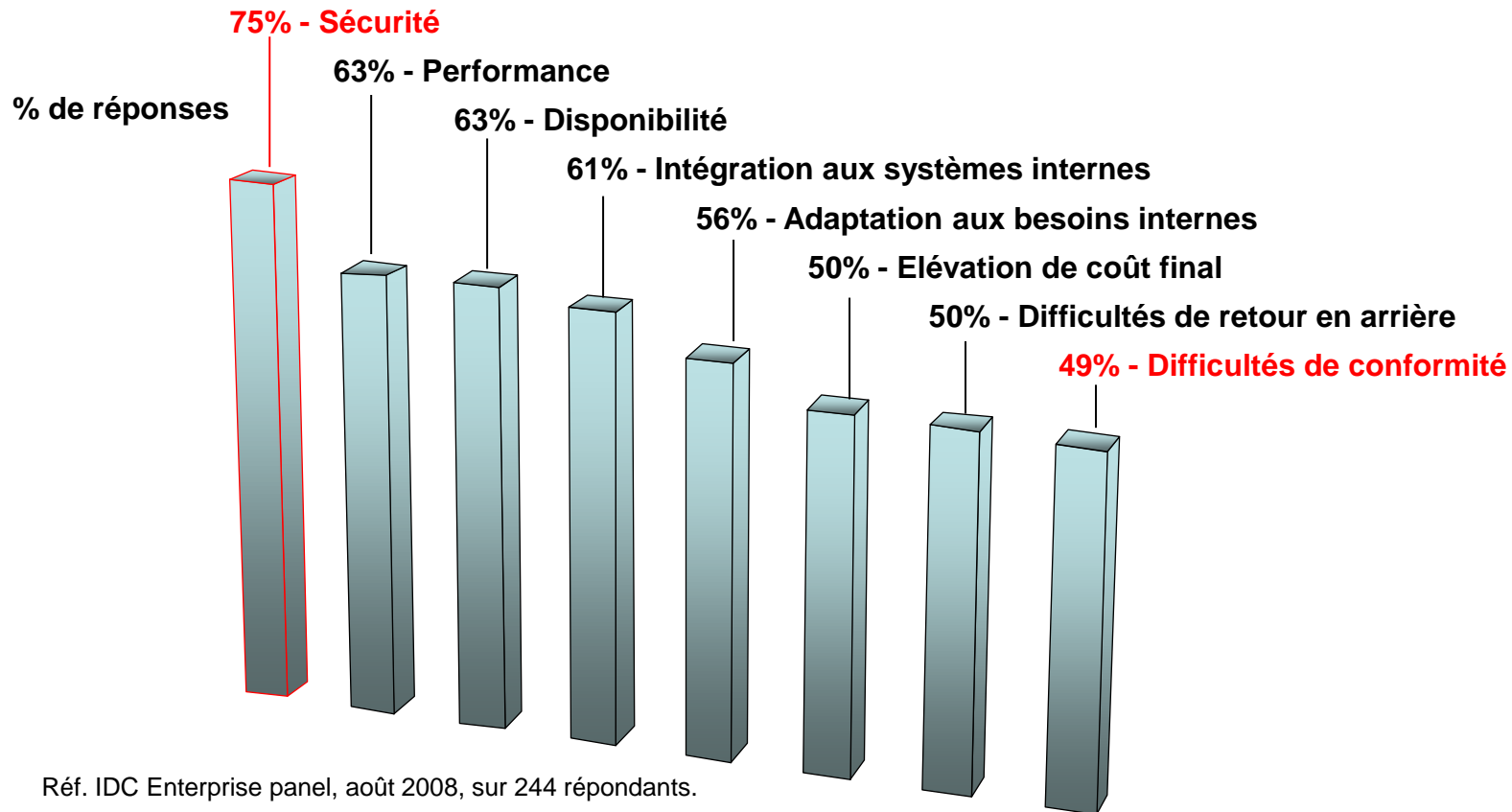
Réf. Y.-T. Chiu (2010) : IEEE Spectrum, vol 47, n° 8, août, p. 11

Des centaines de milliards de dollars seront investis, dont environ 10% en R&D.

La sécurité du "cloud computing"

La sécurité reste le défi majeur

- Défis vus comme les plus significatifs liés au "cloud computing"



La sécurité est largement pressentie comme très préoccupante pour les entreprises.

Menaces liées au "cloud computing"

- Abus ou utilisation non autorisée de services
- Mauvaises configurations
- Interfaces non sûres : API et autres
- Malveillance interne à chaque service
- Problèmes liés au partage d'infrastructure
- Cohabitation de politiques de sécurité différentes
- Perte ou fuite de données
- Détournement de comptes ou de services
- Menaces classiques propagées
- etc.

La concentration des ressources introduit des risques pour la sécurité, mais favorise cependant le contrôle du périmètre et de l'accès physique à meilleur marché par unité.

Niveau d'exposition aux risques

☐ Risques potentiels (35 risques au total)

- 24 risques spécifiques au "cloud computing"
- 11 risques non spécifiques

☐ Catégories de risques spécifiques

- juridiques 4
- organisationnels et politiques 7
- techniques 13

☐ Exposition aux risques

- fonction de l'impact et de l'occurrence
- échelle de niveau : *de faible à fort*
- présentation sur un damier

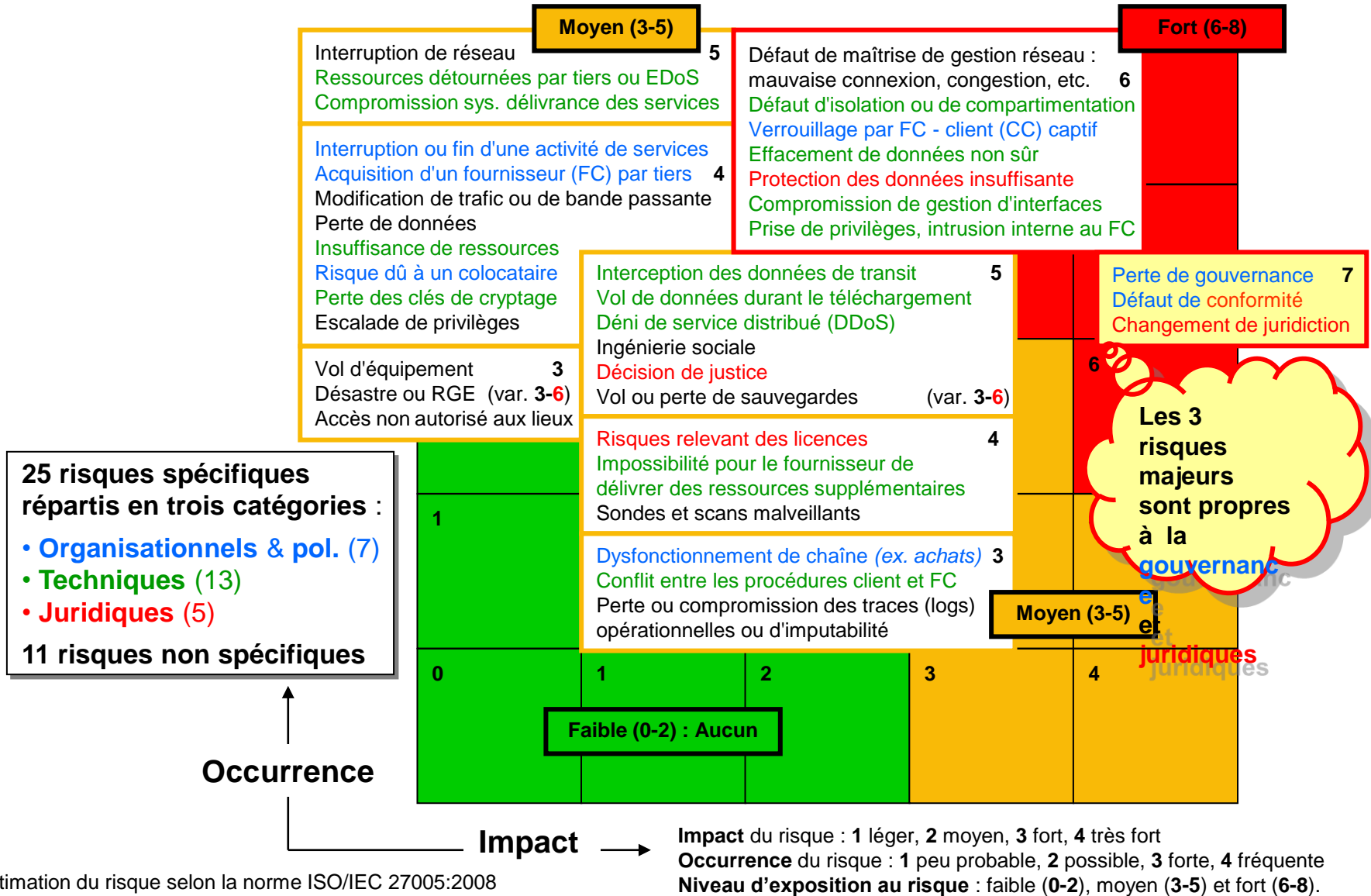
Fort (6-8)

Moyen (3-5)

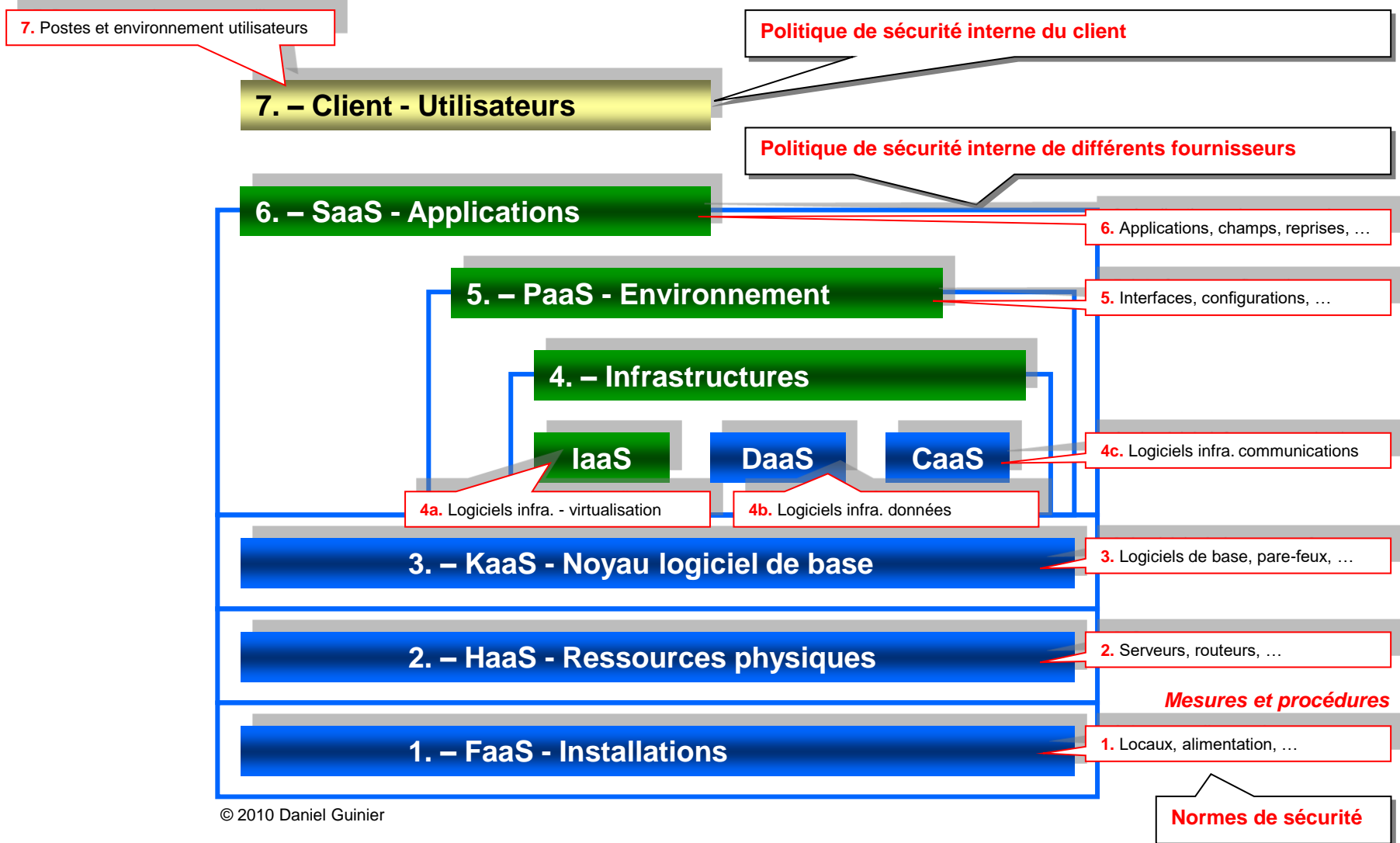
Faible (0-2)

Estimation du risque selon la norme ISO/IEC 27005:2008

Niveau d'exposition aux risques



Sécurité appliquée au modèle général



La cohérence des politiques et mesures est essentielle.

Conclusion

□ Une solution pour les PME en temps de crise

- utilisation d'applications moins coûteuse
- développements plus rapides et moins coûteux
- aucun besoin d'infrastructure et moins en ressources

□ Mais ...

- migration prudente
- sécurité et normes
- garanties à court et long termes

En France, OVH Roubaix a dépassé le cap de **50 000 serveurs** dédiés et propose l'hébergement en "nuages".

(*) Contre 58,6 en 2009 et 68,3 en 2010 (Source : Gartner)

□ Prospective

- environ **2 millions de serveurs** sont déjà "chez Google"
- marché des services (CC) estimé à **149 milliards de dollars en 2014** (*)
- à court terme 25% des serveurs seront dans des **méga-centres**
- à long terme 80% des serveurs seront "en nuages"
- la **sécurité, les télécommunications et l'énergie** sont cruciales

Une solution s'il existe des assurances contractuelles quant aux données, au retour en arrière et à la sécurité, alors que des milliards de \$ sont investis dans des méga-centres.

***Pour l'informatique "... Maintenant ce n'est pas la fin.
Ce n'est même pas le commencement de la fin.
Mais c'est, peut-être, la fin du commencement ..."***

Maintenant en pratique avec les tables rondes

Cet extrait du discours de Winston Churchill du 10/11/42 apparaît adapté à la situation que rencontre l'informatique de plus en plus influencée par les modèles économiques.